Incident Response and Network Forensics Boot Camp

Learn how to detect and respond to security incidents! This popular boot camp builds your knowledge around network forensics and incident response with hands-on labs and expert instruction.

Course description

Infosec's Incident Response and Network Forensics Boot Camp covers the essential information you need to properly detect, contain and mitigate security incidents. You'll learn the ins and outs of incident response as well as the tools used by incident responders on a daily basis. You'll gain hands-on experience in how systems are compromised and what traces are left behind by attackers on the network, on disk and in volatile memory.

Security incidents are a way of life in the modern world, and how organizations respond to them makes a massive difference in how much damage is ultimately done. This boot camp addresses cutting-edge attack vectors as well as tried-and-true methods for compromise. You leave with the knowledge of how to prevent incidents and the skills to defend against a security incident if it does happen.

Who should attend

» Incident response professionals
» Network and system administrators
» Computer security incident response team (CSIRT) members
» Anyone interested in improving their network forensics and incident management skills

Boot camp at a glance

<table>
<thead>
<tr>
<th>Hands-on training</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practice your skills with hands-on labs</td>
</tr>
<tr>
<td>Perform vulnerability analysis and identify rogue processes</td>
</tr>
<tr>
<td>Conduct triage, improve systems, report on findings and more!</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Delivery methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
</tr>
<tr>
<td>In person</td>
</tr>
<tr>
<td>Team onsite</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Training duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immediate access to Infosec Skills</td>
</tr>
<tr>
<td>5-day boot camp</td>
</tr>
<tr>
<td>90-day extended access to all boot camp materials</td>
</tr>
</tbody>
</table>
The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today’s cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you’ll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to hone your skills.

What’s included

» Five days of expert, live Incident Response and Network Forensics training
» 100% Satisfaction Guarantee
» Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
» 90-day extended access to all boot camp video replays and materials
» Pre-study learning path
» Hands-on cyber ranges and labs
» Knowledge Transfer Guarantee

Prerequisites

One or more years of experience in incident handling or equivalent information security experience is recommended.
Course objectives
This boot camp focuses on teaching you the five key incident response steps:
» Plan – Preparing the right process, people and technology enables organizations to effectively respond to security incidents
» Identify – Scoping the extent of the incident and determining which networks and systems have been compromised; includes assessing the extent to which systems have been compromised
» Contain – Prevent the incident from further escalating using information gathered in the previous stage
» Eradicate – Remove intruder access to internal and external company resources
» Recover – Restore fully operational system capability and close out incident

Learn from experts
We don't just have great instructors, our instructors have years of industry experience and are recognized as experts. Over the past 15 years, we've helped tens of thousands of students get certified and advance their careers.

What you'll learn
» The incident response process
» Building an incident response kit
» Event/incident detection
» Categorizing and prioritizing events
» Sources of network evidence
» TCP reconstruction
» Flow analysis
» NIDS/NIPS
» Vulnerability analysis
» Log analysis
» Firewall log investigation
» Log aggregation
» Network artifact discovery
» Identifying rogue processes
» DNS forensics and artifacts
» NTP forensics and artifacts
» HTTP forensics and artifacts
» HTTPS and SSL analysis
» FTP and SSH forensics
» Email protocol artifacts
» Wireless network forensics
» Defensive review
» Secure credential changing
» Reporting and coordinating incidents

Skill up and get certified, guaranteed

100% Satisfaction Guarantee
If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

Knowledge Transfer Guarantee
If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.
What our students are saying

I really appreciate that our instructor was extremely knowledgeable and was able to provide the information in a way that it could be understood. He also provided valuable test-taking strategies that I know not only helped me with this exam, but will help in all exams I take in the future.

Michelle Jemmott
Pentagon

Excellent! Our instructor had a vast background and related the materials to real life. Much better than just teaching the materials to pass an exam ... but he did that as well. He went out of his way in class. The extra materials really benefited us when we returned to our real jobs! Great experience!

John Peck
EPA

Very impressed with Infosec. My instructor did a great job delivering the information strategically and in a way for all to understand. I would definitely take another class/certification prep course.

Sylvia Swinson
Texeltek

The instructor was able to take material that prior to the class had made no sense, and explained it in real world scenarios that were able to be understood.

Erik Heiss
United States Air Force

The course was extremely helpful and provided exactly what we needed to know in order to successfully navigate the exam. Without this I am not confident I would have passed.

Robert Caldwell
Salient Federal Solutions
IR and Network Forensics Boot Camp details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

<table>
<thead>
<tr>
<th>Morning session</th>
<th>Day 1</th>
<th>Day 2</th>
<th>Day 3</th>
<th>Day 4</th>
<th>Day 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>Incident response process (i)</td>
<td>Event &amp; incident detection (i)</td>
<td>Triage &amp; analysis (i)</td>
<td>Incident management knowledge base (i)</td>
<td>Incident response</td>
</tr>
<tr>
<td>Afternoon session</td>
<td>Incident response process (ii)</td>
<td>Event &amp; incident detection (ii)</td>
<td>Triage &amp; analysis (ii)</td>
<td>Incident management knowledge base (ii)</td>
<td>Course materials review</td>
</tr>
<tr>
<td>Evening session</td>
<td>Optional group &amp; individual study</td>
<td>Optional group &amp; individual study</td>
<td>Optional group &amp; individual study</td>
<td>Optional group &amp; individual study</td>
<td></td>
</tr>
</tbody>
</table>

Schedule may vary from class to class

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

During your boot camp

Day 1

Plan
- Incident response planning fundamentals
- Building an incident response kit
- Incident response team components
- IR toolkits and appropriate implementation
- Threat Intelligence
- Cyber Kill Chain
- Agent-based IR

Identify
- Indications of an incident
- Triage
- Critical first steps
- Understanding chain of custody

Contain
- Documentation

Day 2

Event/incident detection
- Written documentation and supporting media evidence
- Identification methods
- Isolation technical procedure best practices
- Containment
- Quarantine considerations for business continuity

Eradicate
- Eradication testing and the QA role
- Incremental backup compromise detection
- Operating system rebuilds

Recover
- Stakeholder identification in recovery process
- Post incident heightened monitoring tasks
- Special actions for specific incident types
- Incident record keeping
- Lessons learned

Constructing your live incident response toolkit
- Trusted command shells – Windows/Linux
- Remote shells
- PsExec vs PowerShell
Limit incident effect and repair incident damage
Perform real-time incident response tasks
Determine the risk of continuing operations
Spearphishing and APT attacks

Sources of network evidence
3 evidence collection modalities
Persistence checks
Sensors
Evidence acquisition
Forensically sound collection of images

TCP reconstruction
TCP session reconstruction
Payload reconstruction
Encapsulation methods
tcpdump/Wireshark
Working with pcap files
Wireshark filtering
Identify missing data
Identify sources of information and artifacts
Packet analysis

Flow analysis
nfcapd and nfdump
nfsen
SiLK
Flow record export protocols
Network file carving
Encrypted flow analysis
Anomalous behavior analysis
Flow data points

NIDS/NIPS
Snort
Snort rule configuration
Collect incident data and intrusion artifacts

Log analysis
Syslog server
Syslog protocol format
Event investigation
Microsoft event log
Event viewer
Modeling analysis formats
HTTP server logs

Apache vs IIS
Header analysis and attack reconstruction

Firewall log investigation
Log formats
iptables and packet flow

Log aggregation
SIEM tools
Splunk architecture

Day 3

Triage & analysis
Categorizing events
Developing standard category definitions
Perform correlation analysis on event reports
Event affinity
Prioritize events
Determining scope, urgency, and potential impact
Assign events for further analysis, response, or disposition/closure.
Determine cause and symptoms of the incident

Network artifact discovery
Network forensics with Xplico

DNS forensics and artifacts
DNS tunneling
Fast flux forensics

NTP forensics and artifacts
Understanding NTP architecture
NTP analysis
NTP usage in timeline analysis and log monitoring
Protocol inspection

HTTP forensics and artifacts
Artifact discovery
Request/response architecture
HTTP field analysis
HTTP web services
AJAX
Web services

HTTPS and SSL analysis
Artifact from secure negotiation process
Other non HTTPS SSL analysis
FTP and SSH forensics
» Capture and inspection
» SFTP considerations

Email protocol artifacts
» SMTP vs POP vs IMAP artifacts
» Adaptations and extensions
» Microsoft Protocols
» Architecture and capture
» Exchange considerations
» SMB considerations
» Cloud email forensics

Wireless network forensics
» Wireless monitoring and capture methodologies
» Understanding Wi-Fi common attacks
» WEP vs WPA vs WPA2
» Wi-Fi security compromise analysis

Perform vulnerability analysis
» Determine the risk, threat level or business impact of a confirmed incident.

Day 4

Timeline analysis
» Timeline reconstruction
» Benefits of structured timeline analysis
» Required pre-knowledge
» Pivot point analysis
» Contexting with incomplete data
» Enter information into an operations log or record of daily operational activity.
» Filesystem considerations
» Time rules
» Using Sleuthkit and fls
» Program execution file knowledge
» File opening and file deletion
» log2timeline
» log2timeline input and output modules
» Using l2t_process for filtering

Volatile data sources and collection
» System memory acquisitions from Windows systems
» 64 bit Windows memory considerations
» Page File analysis
» Hibernation file analysis
» Identify rogue processes
» DLL analysis
» Handle discovery and analysis
» Code injection artifacts Rootkit indicators
» Correlation with network artifacts
» Volatility walk-through
» Redline analysis
» Volatility basics
» Volatility case study
» Advanced malware hunting with Volatility
» Examine Windows registry in memory
» Investigate windows services
» Cached files in RAM
» Credential recovery in RAM

Day 5

Incident response
» Defensive review and recommendations
» Improving defenses
» Secure credential changing process and monitoring
» Increased monitoring period – when and how long
» Validate the system.
» Identify relevant stakeholders that need to be contacted
» Communications about an organizational incident
» Appropriate communications protocols and channels
» Coordinate, integrate and lead team responses with other internal groups
» Provide notification service to other constituents
» Enable constituents to protect their assets and/or detect similar incidents.
» Report and coordinate incidents with appropriate external organizations
» Liaison with law enforcement personnel
» Track and document incidents from initial
» Assign and label data according to the appropriate class or category of sensitivity
» Collect and retain information on all events/incidents in support of future analytical efforts and situational awareness
» Perform risk assessments on incident management systems and networks
» Run vulnerability scanning tools on incident management systems and networks
» CERT-CSIH Review
» CSIH Domains
» CSIH Practice Exam

**After your boot camp**

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

---

**About Infosec**

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at [infosecinstitute.com](http://infosecinstitute.com).